VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

TECHNOLOGIE BLOCKCHAIN A JEJÍ VYUŽITÍ
BLOCKCHAIN TECHNOLOGY AND ITS USE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lukáš Hrbotický**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Václav Zeman, Ph.D.**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Lukáš Hrbotický ***ID:*** 173657
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Technologie blockchain a její využití

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je poskytnout přehledný a komplexní obraz o technologii „blockchain“, popsat její fungování, výhody i nevýhody a provést rozbor jejího praktického nasazení v různých odvětvích. V praktické části práce proveďte rozbor a zhodnocení dostupných „open-source blockchain frameworku“. Na základě uvedeného rozboru navrhněte a realizujte výukovou aplikaci, která bude demonstrovat funkci „blockchainu“ a jejího využití pro konkrétní případ.

DOPORUČENÁ LITERATURA:

[1] BÖHM, Christoph a HOFER, Maximilian. Physical unclonable functions in theory and practice. Springer Science & Business Media, 2012.

[2] PAPPU, Ravikanth. Physical one-way functions. 2001. PhD Thesis. Massachusetts Institute of Technology.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá problematikou technologie blockchain a jejího praktického využití, především v nefinančních službách. Práce popisuje technologii jako takovou a také na ni nahlíží z právního hlediska. Dále uvádí případy praktického nasazení technologie blockchain. V praktické části je návrh dvou laboratorních úloh, kdy se student blíže seznámí s technologií blockchain a realizuje praktické aplikace postavené na této technologii.

KLÍČOVÁ SLOVA

Technologie blockchain, laboratorní úloha, katastr nemovitostí, Exonum, NoobChain

ABSTRACT

This diploma theses concerns the matter of blockchain technology and its practical use, especially for nonfinancial services. Theoretical part describes the blockchain technology from the technological and juridical point of view and examples of its practical use are also mentioned. In the practical part two laboratory exercises were designed for further familiarization of the blockchain technology, in which students try some real applications on their own.

KEYWORDS

Blockchain technology, laboratory exercise, land registry, Exonum, NoobChain

HRBOTICKÝ, Lukáš. *Technologie blockchain a její využití*. Brno, , 45 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Technologie blockchain a její využití“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu práce doc. Ing. Václavu Zemanovi, Ph.D. za cenné rady, metodickou, odbornou a trpělivou pomoc při zpracování diplomové práce.

Obsah

Úvod **9**

1 Technologie blockchain **10**
1.1 Centralizovaná síť . . . 10
1.2 Decentralizovaná síť . . . 11
1.3 Ověřování transakcí . . . 11
1.4 Dokazování hodnoty . . . 13

2 Právní aspekty **14**
2.1 Ověřování akademických listin na Maltě . . . 14
2.2 Katastr nemovitostí . . . 15
2.3 Realitní kanceláře . . . 15
2.4 Ochrana osobních údajů . . . 15
2.5 Shrnutí . . . 16

3 Praktické nasazení blockchainu **17**
3.1 Katastr nemovitostí v Gruzii . . . 17
3.2 Ověřování akademických listin na Maltě . . . 17
3.3 Transakce s nemovitostmi ve Švédsku . . . 19
3.4 Decentralizovaná identita ve Švýcarsku . . . 21
3.5 Správa infrastruktury v Lucembursku . . . 21

4 Open-source blockchain frameworky **24**
4.1 Ethereum . . . 24
4.2 Hyperledger Fabric . . . 24
4.3 Quorum . . . 25
4.4 Corda . . . 25
4.5 NoobChain . . . 25
4.6 Zhodnocení . . . 25

5 Návrh laboratorní úlohy – práce s frameworkem Exonum **26**
5.1 Cíl úlohy . . . 26
5.2 Úkoly . . . 26
5.3 Teoretický úvod . . . 26
5.3.1 Technologie blockchain . . . 26
5.3.2 Využití v praxi . . . 26
5.4 Pracovní postup . . . 27
5.5 Závěr . . . 32

6 Návrh laboratorní úlohy – práce s knihovnou NoobChain **33**
6.1 Cíl úlohy 33
6.2 Úkoly 33
6.3 Teoretický úvod 33
6.3.1 Technologie blockchain 33
6.3.2 Využití v praxi 33
6.4 Pracovní postup 34
6.5 Závěr 40

Závěr **41**

Literatura **42**

Seznam obrázků

1.1 Schema centralizované sítě 10
1.2 Schema distribuované sítě 11
1.3 Schema decentralizované sítě 12
1.4 Schema řetězení bloků 12
3.1 Katastr nemovitostí v Gruzii 18
3.2 Ověřování akademických listin na Maltě 19
3.3 Transakce s nemovitostmi ve Švédsku 20
3.4 Decentralizovaná identita ve Švýcarsku 22
3.5 Správa infrastruktury v Lucembursku 23
6.1 Struktura zdrojových souborů projektu 35
6.2 Grafické rozhraní aplikace 37
6.3 Možná hlášení aplikace o výsledku proběhlé kontroly 39

Úvod

Cílem této diplomové práce je poskytnout přehledný a komplexní obraz o technologii blockchain, popsat její fungování, výhody i nevýhody a provést rozbor jejího praktického nasazení v různých odvětvích. Dále bude vybrán open-source framework, který bude použit v rámci laboratorní úlohy pro aplikaci demonstrující funkci blockchainu.

V první kapitole je seznámení se s technologií blockchain. Následující kapitola nahlíží na problematiku blockchainu z právního hlediska. Následující kapitola popisuje případy praktického nasazení této technologie v různých nefinančních odvětvích. Další kapitola je přehledem nejznámějších open-source frameworků a jejich stručný popis. Poslední dvě kapitoly jsou návrhem laboratorních úloh, kde je kladem důraz na seznámení studentů s principem činnosti technologie blockchain.

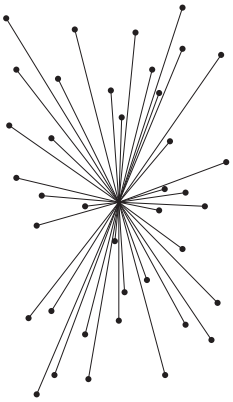
1 Technologie blockchain

Technologie blockchain obvykle odkazuje na transparentní a veřejně přístupnou účetní knihu, která umožňuje bezpečný převod jednotek cenin pomocí šifrování veřejným klíčem a pomocí proof-of-work (hodnota platebního prostředku se dokazuje vynaloženou prací). [27]

První úspěšnou implementací technologie blockchain se stala síť Bitcoin. Z tohoto důvodu si také drtivá většina lidí spojuje pojem blockchain výhradně jen s kryptoměnami. Avšak potenciál blockchainu není omezen jen na Bitcoiny. Technologie, jako taková, si získala mnoho pozornosti v nejrůznějších odvětvích průmyslu včetně finančních služeb, charitativních a neziskových organizacích, umění a elektronického obchodu. [40] [10]

1.1 Centralizovaná síť

Klasický hotovostní platební systém je stále více vytlačován moderním elektronickým, který zahrnuje kreditní a debetní karty, internetové bankovnictví, elektronické obchodování a jiné. Všechny tyto entity jsou centralizované. To znamená, že existuje jedna centrální autorita; servery vlastněné institucemi jako jsou banky, vlády, společnosti vydávající platební karty a další. Při zpracovávání elektronických plateb se tak musí lidé spoléhat na své elektronické produkty jako na důvěryhodné třetí strany. Všechny tyto platební systémy fungují dobře a nabízejí např. ověřování totožnosti anebo digitální podpisy. Nicméně slabinou celého modelu je problém spojený s centrálními platebními systémy. Finanční instituce mohou být napadnuty hackery, převod peněz napříč zeměmi je pomalý, vyžadují vysoké poplatky a zcela se nemohou vyhnout nevratným transakcím. Schema centralizované sítě je znázorněno na obr. 1.1. [36]



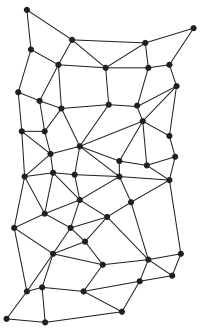
Obr. 1.1: Schema centralizované sítě

1.2 Decentralizovaná síť

V dnešní době již existují protokoly pro decentralizované platební systémy (jako je např. Bitcoin a další kryptoměny). Toto lidem umožňuje navázat pomocí peer-to-peer elektronických peněžních systémů důvěru a provádět transakce bez potřeby třetí strany. Není centrálně ovládána bankou, společností nebo vládou. Čím větší se síť stává, tím je decentralizovanější a zároveň bezpečnější. [25]

Blockchain je základní technologie, která díky spolupráci mnoha počítačů a kryptografii umožňuje navázat důvěru nejen u velkých institucí. Každá jednotlivá transakce (v případě kryptoměn) je odeslána a náhodným uživatelem ověřena. Tímto vzniká rostoucí seznam důvěryhodných záznamů, bloků. Jednotlivé bloky jsou pomocí kryptografických nástrojů spojeny a vytváří globální distribuovanou „účetní knihu“, kterou může kdokoli a kdykoli v síti ověřit. Tímto způsobem se síť vyhýbá centrální autoritě, která může být zkorumpovaná nebo čelit útokům. [12]

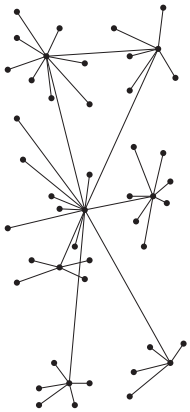
Jednotlivé kryptoměny se v mnoha významech vzájemně liší. Avšak technologie blockchain není zdaleka jen o kryptoměnách. Existuje mnohem více případů využití této technologie než jen v oblasti digitální hotovosti. Schema distribuované sítě je znázorněno na obr. 1.2, zatímco schema decentralizované sítě, která je podmnožinou distribuovaného systému, je znázorněno na obr. 1.3. [36]



Obr. 1.2: Schema distribuované sítě

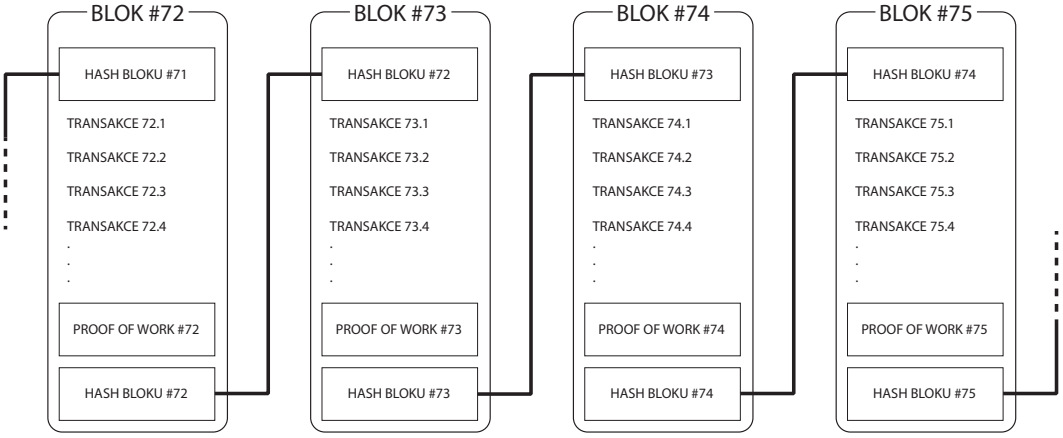
1.3 Ověřování transakcí

Proces potvrzování transakcí se nazývá těžení a lidé, kteří verifikaci provedli, se pak nazývají těžaři. [8] Těžba se používá k zabezpečení a ověření transakcí (ať už těch týkajících se kryptoměn, např. Bitcoinu, nebo jakýchkoli jiných záznamů). Těžba



Obr. 1.3: Schema decentralizované sítě

zahrnuje těžaře, kteří přidávají data o transakcích do globální veřejné knihy provedených transakcí. V těchto knihách jsou bloky zabezpečeny těžaři a jsou vzájemně spojeny a vytvářejí řetězec. Příklad řetězení je znázorněn na obr. 1.4. [16] [17]



Obr. 1.4: Schema řetězení bloků

Bitcoinové transakce jsou ověřovány v decentralizovaných systémech (čímž se liší od tradičních centrálních finančních ústavů), kde lidé přispívají svými výpočetními zdroji k jejich ověření. Proces ověření je nazvaný těžba pravděpodobně podle obdoby těžby komodit – zlata. Těžba zlata vyžaduje hodně úsilí a zdrojů a je zde jen omezená nabídka zlata. [39]

O tom, kdo provede ověření transakce se může soutěžit. Vyhraje ten, kdo transakci ověří nejrychleji, zpravidla tedy těžař s nejvyšším výpočetní výkonem. Tento těžař je následně finančně odměněn. Druhou možností je, že ověření transakce (těžbu)

provede ten, kdo ji sám zadal. [3]

1.4 Dokazování hodnoty

Způsobů, jak prokázat hodnotu dané kryptoměny, existuje několik. Nejčastěji se setkáme se systémy proof-of-work a proof-of-stake. Níže jsou uvedeny i další, méně známé systémy. Nemusíme se však omezovat pouze na kryptoměny. Vytěžit blok blockchainu je třeba v každé jeho aplikaci, tudíž se s těmito metodami prokazování „hodnoty“ setkáváme i mimo finanční aplikace. [11]

Proof-of-work (PoW): hodnota platebního prostředku je prokazována uživatelem pomocí práce (výpočetního výkonu) vynaložené na vytěžení bloku.

Aby se předcházelo stavům, kdy bude daná transakce zaznamenána vícekrát, proběhne hlasování o tom, kdo blok našel. Těžař má větší šanci, že blok objevil právě on, čím větší výpočetní výkon má. V praxi se těžaři shlukují do skupin (mining poolů), čímž získají větší celkový výpočetní výkon. Zvyšují tak svou šanci na odměnu za nalezení bloku, kterou si následně rozdělí podle podílu na celkovém výpočetním výkonu. [28]

Proof-of-stake (PoS): systém je založen na hlasování o prokázání množství vlastněné kryptoměny pro vytváření bloků. [9]

Princip vytváření bloků je založen tak, aby se předcházelo vícenásobnému utrácení. Dosáhneme toho tak, že provedeme hlasování o tom, kdo objevil poslední blok. Čím větší množství a čím déle danou kryptoměnu uživatel vlastní, tím získává větší šanci, že odměnu z objeveného bloku dostane právě on. Z tohoto důvodu jsou kryptoměny založené na systému proof-of-stake výhodné zejména pro investory, neboť lze vydělávat pouze tím, že uživatel vlastní danou kryptoměnu. [26]

Proof-of-concept: jedná se o realizaci jisté metody nebo myšlenky za účelem prokázat její proveditelnost. Případně demonstrovat, že některý koncept nebo teorie má praktický potenciál. [9]

Proof-of-authority: algoritmus poskytující poměrně rychlé transakce prostřednictvím mechanismu konsensu založeného na identitě jakožto opěrnému bodu. [9]

Proof-of-space: uživatel zpřístupní nezanedbatelné množství paměti poskytovateli služby k vyřešení problému, aby tím prokázal legitimní zájem o službu. [9]

2 Právní aspekty

Specifická právní úprava, která by upravovala technologii blockchain, neexistuje. Psát zákon o blockchainu by nebylo efektivní. Na druhou stranu existuje nespočet publikací a akademických diskusí, neboť se jedná o aktuální a velmi populární téma. Musíme si však uvědomit, že se jedná pouze o akademické diskuse. Konkrétní zákon však neexistuje. V obecné rovině nemůžeme stanovit výčet pro oblast právo a blockchain. Vždycky záleží na tom, kde se tato technologie použije, v jaké oblasti, a následně nám dané užití generuje konkrétní právní agendu. [19] [21]

Blockchain se používá ve finančních službách, někde se touto technologií vedou zdravotnické záznamy, zpracování potravin atd. Rozmach blockchainu je v poslední době enormní, tudíž se jeho nasazení objevuje ve spoustě oblastí. Tudíž, pokud chceme uvažovat o právních aspektech, tak je potřeba nejprve konkretizovat oblast použití a pak můžeme o těchto právních aspektech uvažovat. Právní aspekty blockchainu, jako takového, neexistují. To je všechno a nic. To může zahrnovat smlouvy, chytré smlouvy, to může být odpovědnost, moderní katastr nemovitostí, správní regulace, pokud to použijeme v mezinárodní přepravě, tak je to regulace přepravy. Je potřeba se dívat na tu konkrétní aplikaci. O použití blockchainu se mluví v souvislosti s evidencí zdravotnické dokumentace. Zde je třeba myslet na skutečnost, že tato oblast má speciální regulaci, protože zdravotnická dokumentace je regulována specificky, ta má svůj zvláštní režim. [7]

Položme si otázku, zda má takové enormní nasazení technologie blockchain vůbec smysl? Stále není zcela zřejmé, jak se technologie blockchain v těch konkrétních aplikacích chová a už jsou snahy na této technologii stavět všemožné aplikace a vidinou světlé budoucnosti. Tohle všechno je opravdu jen a pouze akademická diskuse, která se do psaného práva, do těch konkrétních pravidel, nedostává. Dokud na to nebudeme mít stanoviska orgánů, soudní rozhodnutí atd., tak všechny aplikace budou provozované v režimu, že fungují, ale stále čekáme na to, až se autoritativně řekne, jestli to opravdu funguje. Tento režim by měl takto fungovat, není proti tomu žádný důvod, ale nemáme pro to žádné stanovisko orgánů, žádná soudní rozhodnutí, která by nám říkala, jak kterou aplikaci realizovat. To většinou přichází až s praxí, bohužel až ex post. [20]

2.1 Ověřování akademických listin na Maltě

Nabízí se položit si otázku: a dává to smysl? Nasazení technologie blockchain má obecně smysl tam, kde chceme zefektivnit daný proces anebo chceme nahradit důvěru v instituci důvěrou v tuto technologii. Tam má nasazení odůvodněný význam. Tam můžeme danou instituci z důvěrností oblasti vyloučit, nemusíme jí důvěřovat,

a důvěřujeme použité technologii, tedy blockchainu. Avšak právě univerzity nepatří mezi příliš nedůvěryhodné instituce. Nasazení blockchainu může v této oblasti naopak přinést i jisté komplikace; někdo musí nad provozem dohlížet, někdo musí instruovat zaměstnance; jak mají nový systém používat, co s ním mají dělat. Co nám aplikace blockchain v této oblasti přinese? Přineslo by to skutečnost, že bychom měli v blockchainu diplomy, které by nešlo revokovat. Přineslo by nám to větší důvěru ve vydané diplomy?

Malta je v tomto ohledu, tedy v zavádění inovací, velmi specifická, neboť těží ze skutečnosti, že jsou na společném trhu a tím se na tento společný trh dostává spousta podnětů, které by se v jiném státě nemohly prosadit. Minimálně ne tak snadno. Na Maltě mají dokonce zvláštní úpravu pro Bitcoin a zvláštní právní předpis upravující virtuální měny. Toto jsou spíše kroky konané s vyhlídkou nalákat investory a dostat se do televize a médií. [20]

2.2 Katastr nemovitostí

Na úvod se opět nabízí filozofická otázka; čeho tím docílíme? Zefektivní se daný proces? Ano, nemusíme důvěřovat danému katastru, ale je tu i druhá stránka věci a to, že je relativně často potřeba zasahovat do záznamů (např. když někdo zpochybní vlastnictví) a revokovat již provedený záznam. Toto nám technologie blockchain ze své podstaty nedovoluje. [18]

2.3 Realitní kanceláře

Daný proces je sám o sobě sice zdokumentovaný a je to jisté, ale když zmanipulujeme vstupní data zvenku vstupující do toho procesu, tak tím, že je tento proces kvalitně technicky ošetřený, můžeme zpochybnit proces jako takový. Zpochybňujeme závěť, objeví se další dědic... V této oblasti bychom zajisté získali jedno velké pozitivum a tím je zefektivnění a zrychlení celého procesu převodu nemovitostí. Avšak opět, stejně jako v předchozím případě, narazíme v případě potřeby revokace či změny již provedeného záznamu. [20]

2.4 Ochrana osobních údajů

Velmi zajímavou otázkou týkající se technologie blockchain je otázka ochrany osobních údajů. V blockchainu je to obecná otázka. Jelikož distributed ledger je distributed, tak nemáme kontrolu nad tím, kde konkrétně se osobní údaje nacházejí, protože

se najednou nacházejí po celém světě. Existuje zvláštní právní agenda, která pojednává o zpracování osobních údajů v rámci Evropské Unie. Jsou stanovena zvláštní pravidla, kdy se osobní údaje nesmějí zpracovávat jinde než v Evropské Unii. A v případě nasazení technologie blockchain nemáme absolutně žádnou kontrolu nad tím, kde všude se daný osobní údaj objeví. Na jednu stranu se opravdu jedná o zpracování osobních údajů, ale na druhou stranu, když dojde na věc, v případě vypracování analýzy rizik zjistíme, že riziko zneužití těchto osobních údajů je naprosto minimální, protože osobní údaje jsou ve většině aplikací vkládány do bloků zašifrované nebo ve formě hashe. Z toho plyne, že toto nakládání s osobními údaji je sice protiprávní, ale reálně, protože tam je minimální riziko, tak je tam minimální nutnost ta data chránit. [20]

2.5 Shrnutí

Je tedy zřejmé, že vývoj technologie blockchain je v právní oblasti teprve v začátcích. Na začátku jsou vždy jistí first runners, kteří buďto uspějí nebo neuspějí. Ti se musejí vypořádat s konkrétní regulativní odezvou, oni se musí vypořádat s tím, jestli svými výsledky přesvědčí lidi, že to bude nebo nebude fungovat, a teprve pak přichází ta druhá generace, která na tom jakoby vydělá. V současné době již tyto first runners máme, ale stále čekáme na tu hlavní vlnu, kteří se to pokusí prolomit. Z hlediska práva to není problém, ale jakým způsobem se potká právo s těmi konkrétními realizacemi, s těmi business modely, to je otázka. [18] [21]

Jak bylo řečeno výše; zákon o blockchainu neexistuje. Řídíme se vždy těmi konkrétními právními předpisy, které souvisejí s tou konkrétní aplikací technologie blockchain. Čili, zajímá nás oblast použití, nikoliv použitá technologie. Jeho masivnější prosazení v praxi bude záležet na prokazatelných výhodách oproti stávajícím řešením.

3 Praktické nasazení blockchainu

Technologii blockchain si drtivá většina lidí spojuje výhradně s kryptoměnami (především s Bitcoinem). To by byl však velmi úzký úhel pohledu, neboť praktické nasazení je daleko širší. V následujících sekcích je tato technologie představená v různých odvětvích, tedy i mimo bankovní sektor. [5] [1]

3.1 Katastr nemovitostí v Gruzii

Správní úřad Gruzínské republiky používá technologii blockchain, aby poskytla svým občanům digitální osvědčení o jejich pozemku. Děje se tak, že přidá kryptografický důkaz o tom, že transakce byla zveřejněna v bitcoinovém blockchainu. Gruzínský správní úřad spolupracuje s Bitfuri Group, která poskytuje řešení založená na protokolu Bitcoin a tento projekt započal v dubnu 2016. Toto Gruzii pomáhá bojovat proti korupci a řešit spory o majetkové nároky. Hlavním důvodem k použití blockchainu je zvýšit důvěryhodnost veřejnosti k vedení záznamů o majetku.

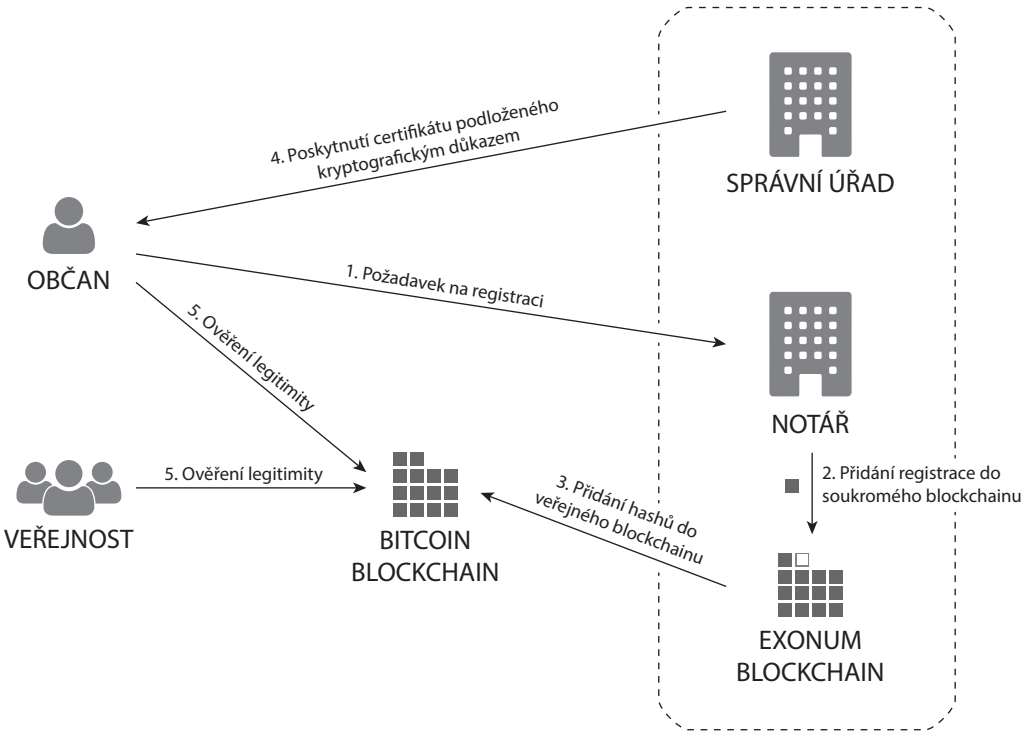
Technologii blockchain používají občané k ověřování certifikátů souvisejících s majetkem a notáři ji používají k vytváření nových registrací. Služba momentálně umožňuje registraci nákupů a prodejů současných pozemků a registraci nových pozemků. Systém je neustále vyvíjen a plánuje se rozšíření o registraci demolicí nemovitostí hypotéky, nájmy a notářské služby.

Framework Exonum je používá k usnadnění projektů, které umožňují organizacím budovat a zpřístupňovat soukromé nebo veřejné blockchainy se zachováním bezpečnosti, kterou blockchain poskytuje. Tento framework umožňuje uživatelům (v tomto případě notářům) ověřovat informace na klientské straně. Také ukládá hashe do bitcoinové sítě, což znemožňuje změnu. Software je open-source. Princip činnosti znázorňuje obr. 3.1.

Soukromá data nejsou uložena ve veřejném bitcoinovém blockchainu. Zde je uložen pouze hash stavu systému. Každý uzel soukromého blockchainu Exonum (správní úřad a notáři) má kompletní a aktuální kopii dat. V případě poškození uzlů postačí k obnovení blockchainu jediný uzel. [33] [34] [14]

3.2 Ověřování akademických listin na Maltě

Maltská vláda spustila v říjnu 2017 projekt, který vyvíjí systém pro ověřování akademických listin využívající blockchain technologii. Maltské Ministerstvo školství a práce se rozhodlo využít Blockcerts, otevřený standard pro správu akademických záznamů. Blockerts zajišťuje všechny aspekty; vytváření, vystavování, prohlížení



Obr. 3.1: Katastr nemovitostí v Gruzii

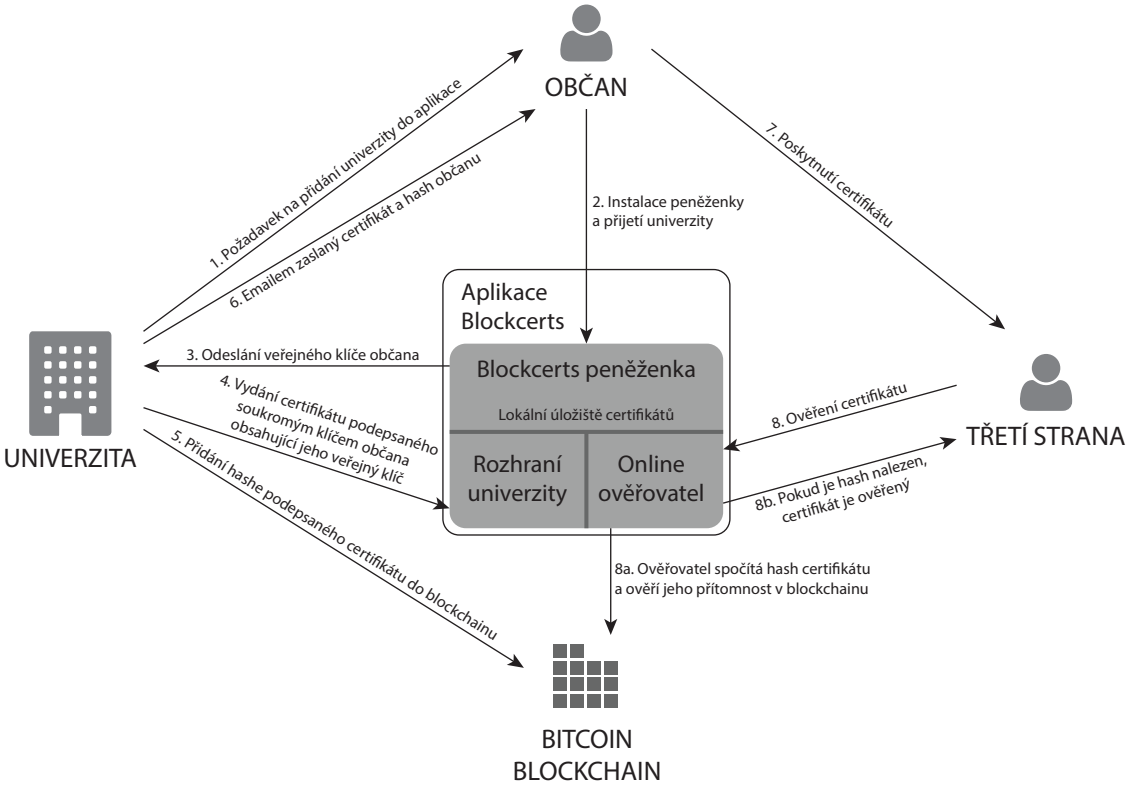
a ověřování certifikátů a využití blockchain technologie jako infrastruktury. Pilotní verze byla zahájena s cílem vytvořit ověřitelný důkaz vzdělání pro občany.

Mezi funkce poskytované v rámci projektu patří vydávání akademických listin, ověřování certifikátů a ukládání osobních údajů v aplikaci uživatele. Aplikace Blockcerts poskytuje peněženku, kde má občan plnou kontrolu nad svými záznamy. Systém občanům umožňuje kontrolovat, které třetí strany mohou vidět a ověřovat originalitu jejich akademických listin. Ověření lze provést pomocí univerzálního webového validátoru *verifier5*. Zadáním URL adresy certifikátu lze ověřit platnost certifikátu, vlastníka listin, datum vydání, vydávající instituci a ID transakce.

Otevřený standard Blockcerts je stále ve vývoji a jelikož se zatím jedná pouze o pilotní nasazení, je projekt malého rozměru. Zahrnuje pouze dvě vzdělávací instituce a jejich studenty. Ověřovací software je implementován v obou institucích a peněženka dává studentům kontrolu nad certifikáty. Škálovatelnost závisí na zvolené blockchainové platformě. Standard Blockcerts vydává hashe do blockchainu v dávkách, což umožňuje škálovatelnost dokonce i na Bitcoinové platformě. Propustnost Bitcoinu je aktuálně sedm transakcí za sekundu, ale dávkování umožňuje větší míru propustnosti. Princip činnosti znázorňuje obr. 3.2.

Blockcerts se skládá z open-source knihoven, nástrojů a mobilních aplikací pro

vytváření, ukládání, sdílení a ověřování osobních certifikátů. Soukromá blockchain síť se bude sestávat výhradně z certifikovaných institucí, které budou v registru akademických certifikátů využívající Blockcerts řešení. Strojové učení se snaží rozšířit integraci standardu na více blockchainových platforem, ale v současnosti se používá pouze blockchain Bitcoin. Do jisté míry je tato situace způsobena tím, že v roce 2015, kdy Blockcerts zahájil svoji činnost, byl Bitcoin jediná stabilní blockchain platforma. V současné době se komunita snaží vytvořit interoperabilitu se systémem Etherum. [22] [23] [31]



Obr. 3.2: Ověřování akademických listin na Maltě

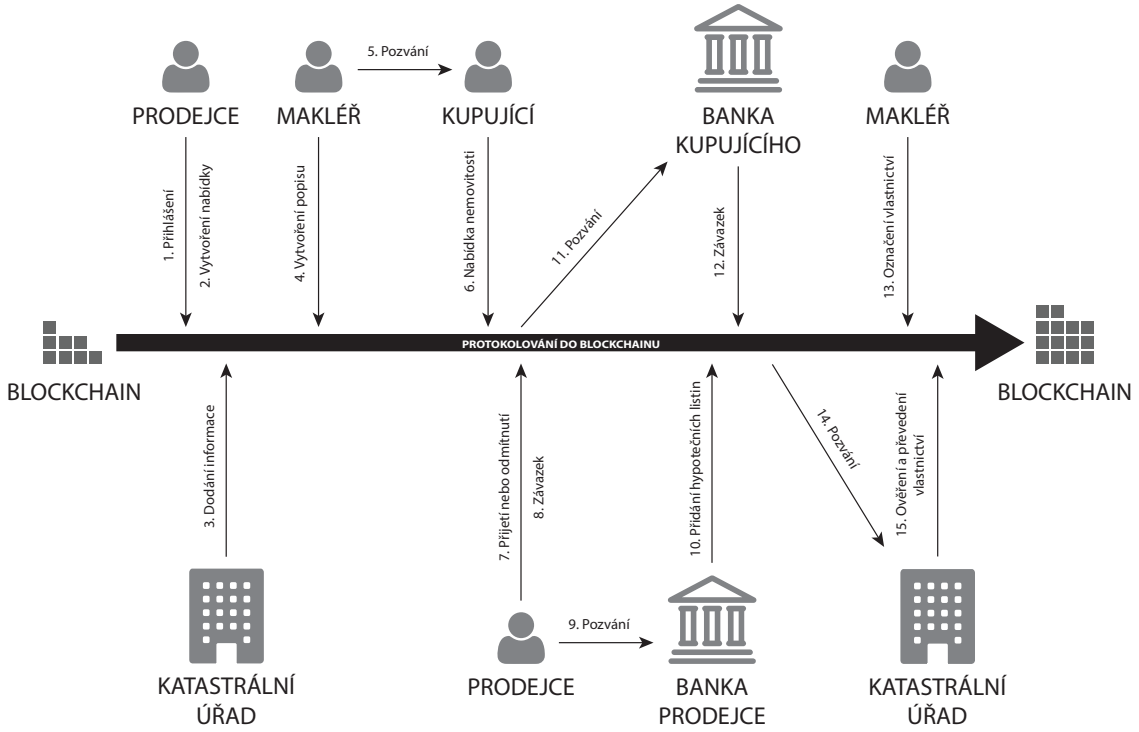
3.3 Transakce s nemovitostmi ve Švédsku

V branži realitních kanceláří se operuje s vysokými částkami, což zdůrazňuje důležitost bezpečnosti a transparentnosti transakcí s nemovitostmi. V současnosti je vyřizování transakcí s nemovitostmi pomalé, finančně nákladné a vystavené obchodním rizikům (např. spory v majetkových listinách). Tento projekt řeší nedůvěru mezi smluvními stranami v oblasti převodu nemovitostí a zvyšuje rychlost transakcí. Projekt byl zahájen v září 2016 švédským úřadem pro mapování a katastr nemovitostí a několika tamními finančními institucemi.

Toto řešení představuje zcela nový pracovní postup založený na blockchainu, který zefektivňuje a zabezpečuje převod vlastnického práva. Systém je propojený se švédským katastrem nemovitostí, který je zodpovědný za správu katastru nemovitostí. Blockchain jen ukládá stav systému po provedení každého jednotlivého kroku pracovního postupu. Tímto je zajištěna synchronizace mezi účastníky zainteresovanými do transakce. V blockchainu je uložena jediná privátní informace a tou je cena prodávajícího. Všechny ostatní informace jsou podle švédské legislativy veřejné.

Projekt je stále v pilotní fázi, přestože již trvá přes tři roky. Konsorcium (uzly patřící do švédského katastru nemovitostí) má sice funkční technologii, ale toto technické řešení dosud není integrováno do prostředí realitních kanceláří. Škálovatelnost není problém, pokud se objem transakcí zvýší, protože uzly mohou zvýšit kapacitu přidáním dalších serverů. Princip činnosti znázorňuje obr. 3.3.

Tento pilotní projekt používá soukromý blockchain systém, který je distribuovanou databází v rámci konsorcia (uzly patřící do švédského katastru nemovitostí). Blockchain systém se nazývá Postchain. Postchain používá databázový systém PostgreSQL, jehož kapacita je dostatečně velká k uložení všech dat v blockchainu. Aby se dodržely regule zákona, tak jsou identifikační údaje uloženy mimo řetězec a v blockchainu jsou reprezentovány hashem. Tento hash odkazuje na dokument obsahující úplné informace. [35] [4]



Obr. 3.3: Transakce s nemovitostmi ve Švédsku

3.4 Decentralizovaná identita ve Švýcarsku

Švýcarské město Zug spustilo vládou publikovaný systém identity nazvaný uPort, který je založený na blockchainu Ethereum. Cílem projektu je poskytnout důvěryhodnou a nezávislou identitu založenou na blockchainu pro autentizaci služeb elektronické správy a sdílení osobních údajů s třetími stranami. Služba uPort umožňuje selektivní zpřístupnění konkrétních informací konkrétním společnostem nebo vládním institucím, což občanům poskytuje úplnou kontrolu nad jejich osobními údaji.

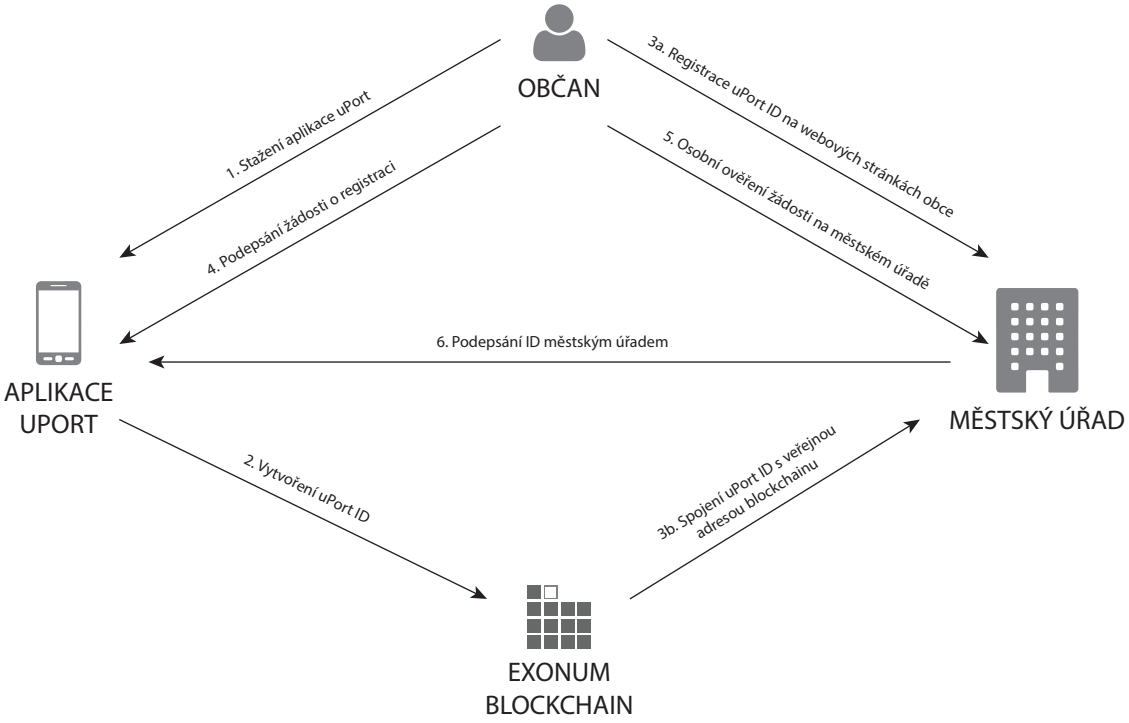
UPort zavádí decentralizovaný model správy a potvrzování identity osob. Dosud jediná veřejná služba, pracující s novou digitální identitou, je důkaz o pobytu. Cílem projektu je rozšíření o další služby provozované místními orgány jako je: průzkumy veřejného mínění, elektronické hlasování, půjčování knih, podávání daňového přiznání nebo poplatky za parkování. Občané si musí zaregistrovat uPort identitu na městském úřadu. Registrační kancelář má v uPort aplikaci administrátorská práva a po ověření, které musí být provedeno osobně na radnici, městský úřad vydá osvědčení podepsané soukromým klíčem, jakožto důvěryhodné vlastnictví pro serverovou stranu. Toto zabezpečí, že uPort identita bude rozpoznána jako oficiální, vládou důvěryhodná, identita.

Projekt byl spuštěn 15. listopadu 2017. V počáteční fázi pilotního projektu se používá testovací síť Etherea Rinkeby a nikoli hlavní síť. Časem bude služba přesunuta z testovací sítě, protože ta poskytuje jen omezené množství uzlů. Ze všech občanů švýcarského Zugu se doposud zaregistrovalo jen 1 % obyvatel (odpovídá asi 300 občanům). Toto množství testovací síť podporuje. Se současnou architekturou by však mohly nastat problémy při škálování na jiné obce. Princip činnosti znázorňuje obr. 3.4.

Z uživatelského pohledu je hlavním bodem interakce se systémem aplikace uPort. Používá se pro ukládání všech osobních údajů do zařízení uživatele. Po instalaci vytvoří aplikace jedinečný soukromý klíč, který je uložený v mobilním zařízení. [30] [42] [24]

3.5 Správa infrastruktury v Lucembursku

Infrachain je nezisková organizace založená v listopadu 2016 v Lucembursku. Cílem je podporovat vytváření nezávislých a nezkorumpovatelných uzlů zapojených do operací instancí blockchainu. Vládou používané rozhraní Infrachain věnuje pozornost ochraně soukromí, kybernetické bezpečnosti, trestnímu stíhání a kontinuitě činností organizace ve stejné míře jako centralizované systémy. Rozhraní si žádá oddělení vrstvy služeb a síťové vrstvy a vytvoření referenční blockchainové infrastruktury složené z nezávislých uzlů hostující různé veřejné a soukromé služby.

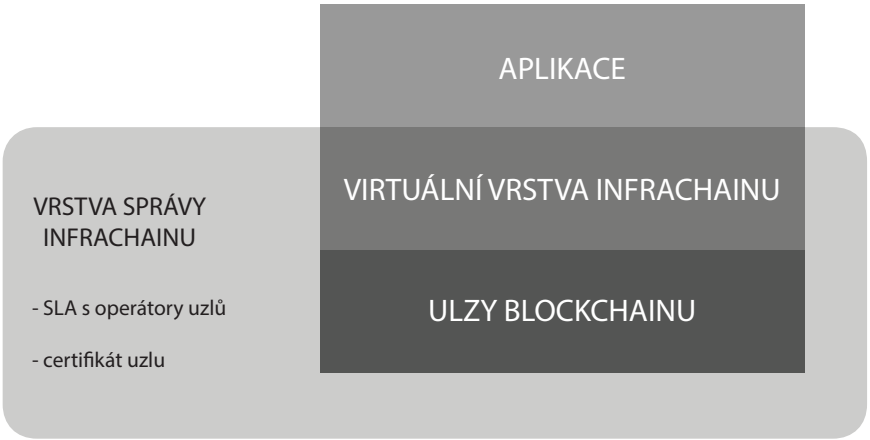


Obr. 3.4: Decentralizovaná identita ve Švýcarsku

Projekt neposkytuje občanům žádnou konkrétní funkcionalitu, přesto iniciuje podněty, jako je automatická koordinace platforem mezi blockchainovými aplikacemi a evropskou sítí nezávislých certifikovaných uzlů.

Projekt je v současné době v pilotní fázi, ale některé případy použití již byly vyzkoušeny na certifikovaných uzlech zakládajících členů Infrachainu. Mnoho funkcí je stále ve vývoji, jako např. umístění do rámce GDPR. Princip činnosti znázorňuje obr. 3.5.

Infrachain používá SLA pro práci s uzly k vytvoření vládní vrstvy, která zvyšuje důvěru a odpovědnost v uzlech, zajišťuje prostředí pro blockchainové projekty a dodržování předpisů. Vládní vrstva se nezaměřuje na žádný konkrétní protokol. Provozovatelé certifikovaných uzlů poskytují SLA společnosti Infrachain a Infrachain poskytuje SLA poskytovatelům aplikací. [6]



Obr. 3.5: Správa infrastruktury v Lucembursku

4 Open-source blockchain frameworky

Pro demonstraci funkce blockchainu bude využito některého z volně dostupného open-source frameworků. Takovýchto řešení se na Internetu nachází hned několik. Některá z nich byla vybrána a v následujících kapitolách popsána. [32]

4.1 Ethereum

Veřejnou síť blockchainů Ethereum vyvinul Vitalk Buterin. Je považována za jednu z nejefektivněji vyvinutých platforem, která má funkce smart contract, flexibilitu a přizpůsobitelnost pro více odvětví průmyslu.

Ethereum funguje jako základní komponenta při vytváření a vývoji většiny decentralizovaných aplikací. Výhody, které Ethereum nabízí oproti jiným aplikacím, jsou především stabilita, bezpečnost, zabezpečení a prevence korupce.

Ethereum nabízí ve srovnání s Hyperledgerem větší transparentnost. Jeho flexibilita umožňuje každému vývojáři vytvářet aplikace pomocí vestavěného programovacího jazyka. Použití Ethera, jakožto vestavěné kryptoměny, nabízí konkurenční výhodu oproti jiným řešením v aplikacích vyžadujících použití kryptoměny. [38] [13]

4.2 Hyperledger Fabric

Hyperledger Fabric je síť poskytující oprávnění registrovat každého uživatele poskytnutím oprávnění přístupu k identitě a transakcím, které budou určovat rozsah oblasti, v níž může ten daný uživatel pracovat a oblasti, kde již bude potřebovat povolení od ostatních uživatelů.

Modulární architektura této platformy z ní dělá jedno z nejlepších řešení pro podnikové nasazení. Přestože nenabízí vestavěnou funkci měny, lze ji podle požadavků vytvořit pomocí řetězových kódů.

Důvěrnosti je dosaženo šifrováním transakcí, které mohou být modifikovány jen oprávněnými osobami. Tato funkce řeší problém Etherea, který nabízí transparentnost bez ohledu na soukromí. Jelikož je postaven na modulárním přístupu, vyžaduje méně úrovní ověřování a tím optimalizuje výkon celého softwaru. Datové části na blockchainu umožňují firmám chránit data, která jsou vysoce citlivá z důvodu nařízení různými zákony, povolením přístupu jen zúčastněným stranám. [2]

4.3 Quorum

Quorum je podniková platforma založená na Ethereu zaměřená na smart contract. Platforma byla vytvořena v roce 2016 zavedením EEA (Ethereum Enterprise Alliance). Podporuje jak veřejné, tak i soukromé transakce. Platforma je ideální pro použití v aplikacích vyžadujících vysokou rychlost a rychlé zpracování soukromých transakcí. Je to vyvíjející se podniková síť blockchainů, která měla úspěšné implementace v průmyslu mimo finanční sektor.

Rychlost zpracování transakcí je vyšší ve srovnání s Ethereem, což je výsledkem jednoduchého mechanismu konsensu. Většinu aktualizací Etherea lze snadno integrovat do Quoruma, protože se jedná o rozšíření této platformy. [29] [41]

4.4 Corda

Corda funguje na konceptu vytvoření globální logické knihy, kde všichni uživatelé, mající nefalešné úmysly, mohou mezi sebou komunikovat a spravovat smlouvy a kontrakty. Původní zájem Cordy o finanční sektor se nyní rozšiřuje i na odvětví vládní, zdravotnické a obchodní. Výhodou je, že se v síti mohou pohybovat jen uživatelé s legitimním zájmem, což zabraňuje neoprávněnému přístupu k databázi. [37]

4.5 NoobChain

Jedná se o jednoduchou, ale velice funkční, implementaci řešení blockchainu určenou primárně pro vzdělávací účely. Tomu také odpovídá přehledný a snadno rozšiřitelný zdrojový kód.

4.6 Zhodnocení

Pro realizaci výukové aplikace byla vybrána řešení Exonum a NoobChain. První zmiňovaný framework je v praxi běžně používaný a umožní studentům nahlédnout k tvorbě reálné aplikace. Naopak NoobChain je tvořený právě pro pedagogické účely. Jeho zdrojový kód je jednoduchý a přehledný, tudíž studenti budou mít větší možnosti při individualizaci aplikace a lépe porozumí podstatě technologie blockchain.

5 Návrh laboratorní úlohy – práce s frameworkem Exonum

5.1 Cíl úlohy

Seznámit se s principem činnosti technologie blockchain. Pochopit princip provádění transakcí a vyzkoušet si vytvořit jednoduchou aplikaci.

5.2 Úkoly

1. Provést instalaci operačního systému Linux ve virtuálním prostředí.
2. Nainstalovat si nástroje potřebné pro vývoj aplikace na framework Exonum.
3. Dle přiloženého návodu naprogramovat praktickou aplikaci.

5.3 Teoretický úvod

5.3.1 Technologie blockchain

Technologie blockchain obvykle odkazuje na transparentní a veřejně přístupnou účetní knihu, která umožňuje bezpečný převod jednotek cenin pomocí šifrování veřejným klíčem a pomocí proof-of-work (hodnota platebního prostředku se dokazuje vynaloženou prací).

5.3.2 Využití v praxi

Technologii blockchain si drtivá většina lidí spojuje výhradně s kryptoměnami (především s Bitcoinem). To by byl však velmi úzký úhel pohledu, neboť praktické nasazení je daleko širší. Odstavce níže uvádějí příklady nasazení blockchainu v praxi. Jedná se pouze o výběr. Obdobných aplikací existuje po celém světě spousta a mnohé další každým dnem vznikají.

Katastr nemovitostí v Gruzii

Správní úřad Gruzínské republiky používá technologii blockchain, aby poskytla svým občanům digitální osvědčení o jejich pozemku. Děje se tak, že přidá kryptografický důkaz o tom, že transakce byla zveřejněna v bitcoinovém blockchainu. Gruzínský správní úřad spolupracuje s Bitfuri Group, která poskytuje řešení založená na protokolu Bitcoin a tento projekt započal v dubnu 2016. Toto Gruzii pomáhá bojovat

proti korupci a řešit spory o majetkové nároky. Hlavním důvodem k použití blockchainu je zvýšit důvěryhodnost veřejnosti k vedení záznamů o majetku.

Ověřování akademických listin na Maltě

Maltská vláda spustila v říjnu 2017 projekt, který vyvíjí systém pro ověřování akademických listin využívající blockchain technologii. Maltské Ministerstvo školství a práce se rozhodlo využít Blockcerts, otevřený standard pro správu akademických záznamů. Blockerts zajišťuje všechny aspekty; vytváření, vystavování, prohlížení a ověřování certifikátů a využití blockchain technologie jako infrastruktury. Pilotní verze byla zahájena s cílem vytvořit ověřitelný důkaz vzdělání pro občany.

5.4 Pracovní postup

1. Provést instalaci operačního systému Linux ve virtuálním prostředí: Nejprve si nainstalujeme virtualizační prostředí. Pro potřeby této laboratorní úlohy zvolíme VMware Workstation 15.5 Pro. Ten si stáhneme z webové adresy: `www.vmware.com`. Provedeme instalaci a následně nainstalujeme libovolnou Linuxovou distribuci. Tento návod popisuje práci v prostředí Ubuntu ve verzi 18.04. Z adresy: `www.ubuntu.cz` si můžeme stáhnout např. zmiňovanou distribuci Ubuntu jako obraz instalačního disku 64bit verze.

Spustíme si VMware a vytvoříme si nový virtuální stroj. Zvolíme: *Player* → *File* → *New Virtual Machine...* nebo použijeme klávesovou zkratku Ctrl+N. V dialogovém okně *New Virtual Machine Wizard* zvolíme možnost *Installer disc image file (iso)* a kliknutím na tlačítko *Browse...* připojíme stažený obraz instalačního disku. Uživatelské jméno a heslo volíme rozumně a snadno zapamatovatelné, nejlépe *User name:* `student` a *Password:* `student`. V reálném nasazení volíme samozřejmě hesla silnější a bezpečnější. Dle pokynů instalačního průvodce dokončíme instalaci a nastavení virtuálního stroje. Po dokončení by se nám měl virtuální stroj ihned spustit. Pokud se tak nestane, spustíme jej stiskem *Play virtual machine*, dokončíme instalaci a přihlásíme se námi zvolenými přihlašovacími údaji zadanými při instalaci.

2. Nainstalovat si nástroje potřebné pro vývoj aplikace na framework Exonum: Funkčnost řešení Exonum je závislá na knihovnách třetích stran; *RocksDB*, *libsodium* a *Protocol Buffers*. V případě, že kdykoliv budeme mít při instalaci problém s oprávněním, budeme informování výpisem do konzole např. takto:

```
student@ubuntu:~/exonum$ cargo test -p exonum
Updating crates.io index
error: failed to write /home/student/exonum/Cargo.lock
```

```
Caused by:
failed to open: /home/student/exonum/Cargo.lock
Caused by:
Permission denied (os error 13)
```

Příkaz tedy zopakujeme s administrátorskými právy:

```
student@ubuntu:~/exonum$ sudo cargo test -p exonum
```

V případě, že bude některý z použitých příkazů chybět (záleží na zvolené distribuci Linuxu), tak budeme informováni např. hláškou:

```
Command 'cargo' not found, but can be installed with:
sudo apt install cargo
```

Doinstalujeme tedy potřebný příkaz pomocí:

```
student@ubuntu:~/exonum$ sudo apt install cargo
```

Nyní začneme s instalací frameworku Exonum a souvisejících nástrojů (v závislosti na zvolené distribuci Linuxu a její verzi volíme i odpovídající verzi knihovny *rocksdb*):

```
add-apt-repository ppa:exonum/rocksdb
apt-get update
apt install librocksdb5.8
apt-get install build-essential libsodium-dev libsnappy-
  ↪ dev libssl-dev librocksdb5.8 pkg-config clang-7 lldb
  ↪ -7 lld-7
```

Instalaci nástroje *protobuf* provedeme pomocí příkazů:

```
add-apt-repository ppa:maarten-fonville/protobuf
apt install libprotobuf-dev protobuf-compiler
```

Pokud náš operační systém již obsahuje předkompilované knihovny, můžeme si nastavit proměnnou prostředí tak, aby ukazovala na adresář s příslušnou knihovnou a tím zkrátit dobu kompilace:

```
export ROCKSDB_LIB_DIR=/usr/lib
export SNAPPY_LIB_DIR=/usr/lib/x86_64-linux-gnu
```

Na závěr nainstalujeme sadu nástrojů programovacího jazyka Rust, kterou využívají repozitáře Exonum:

```
curl https://sh.rustup.rs -sSf | sh -s -- --default-
  ↪ toolchain stable
```

Pokud si chceme ověřit, zda jsme nainstalovali nástroje Rust a potřebné závislosti správně, můžeme spustit předpřipravený test těmito příkazy (tento úkon není pro další postup nutný, test trvá asi 20 minut v závislosti na výkonu počítače):

```
git clone https://github.com/exonum/exonum.git
cd exonum
cargo test -p exonum
```

3. Dle přiloženého návodu naprogramovat praktickou aplikaci: Vývojáři z týmu Exonum nabízejí několik ukázkových příkladů k vyzkoušení. Náš případ, postavený na jednom ze vzorů, bude demonstrovat funkci jednoduchého katastru nemovitostí. Další možnosti, jak si vyzkoušet vlastní aplikaci je např. vytvořit si vlastní kryptoměnu anebo systém sledování pohybu zboží mezi distributory.

Založíme si nový projekt s vhodným název, např. *landregistry*:

```
cargo new landregistry --lib
```

Jelikož by bylo psaní celého zdrojového kódu časově velmi náročné a pro jedince neovládající programovací jazyk Rust zajisté i neefektivní, tak máme připravené torzo zdrojových kódů, které budeme postupně doplňovat. Přestože neovládáme programovací jazyk Rust, snažme se doplňované část zdrojového kódu pročíst a porozumět principu jejich činnosti. Stáhneme si předpřipravené zdrojové kódy a nahrajeme je do složky s vytvořeným projektem.

Rozhraní Protobuf se používá jako formát pro ukládání dat. Datové struktury použité v programu musíme nejprve popsat pomocí Protobuf, od nějž budou generovány datové struktury pro Rust. V našem případě bude datová struktura reprezentovat občana a uvnitř uložené proměnné; veřejný klíč, jméno občana a číslo parcely, kterou vlastní. Do souboru `service.proto` přidáme kód reprezentující datovou strukturu. Zde je prostor pro možné individuální rozšíření funkcionality výsledné aplikace.

```
message Citizen {
  exonum.crypto.PublicKey pub_key = 1;
  string name = 2;
  uint64 plat_num = 3;
}
```

Abychom do projektu integrovali soubory generované Protobufem, přidáme do souboru `mod.rs` tento kód:

```
include!(concat!(env!("OUT_DIR"), "/protobuf_mod.rs"));
use exonum::crypto::proto::*;
```

Do souboru `build.rs` přidáme spustitelnou funkci `main`, která nám na základě předloh z Protobufu vygeneruje Rust soubory:

```
fn main() {
    ProtobufGenerator::with_mod_name("protobuf_mod.rs")
        .with_input_dir("src/proto")
        .with_crypto()
        .generate();
}
```

Nyní si vytvoříme datovou strukturu i v jazyce Rust (soubor `lib.rs`), která se použije pro operace s datovým schematem a k ověření souboru generovaného Protobufem:

```
pub struct Citizen {
    pub pub_key: PublicKey,
    pub name: String,
    pub plat_num: u64,
}
```

Nyní si vytvoříme dvě metody. První slouží ke změně parcelního čísla u daného občana:

```
pub fn change(self, new_num: u64) -> Self {
    let plat_num = new_num;
    Self::new(&self.pub_key, &self.name, plat_num)
}
```

Druhá metoda slouží k odebrání čísla parcely konkrétnímu občanu.

```
pub fn remove(self, new_num: u64) -> Self {
    debug_assert!(self.plat_num == amount);
    let plat_num = 0;
    Self::new(&self.pub_key, &self.name, plat_num)
}
```

Vytvoříme si datovou strukturu reprezentující „transakci“, tedy převod parcely z jedno vlastníka na druhého. Všimněme si, že odpovídá svému vzoru ze souboru `service.proto`.

```
pub struct TxTransfer {
    pub to: PublicKey,
    pub new_num: u64,
    pub seed: u64,
```

```
}
```

Nesmíme opomenout na ošetření chybových stavů při běhu programu. Můžou nastat problémy s neexistujícím uživatelem anebo se špatně zadaným číslem parcely. Pokud nás napadají další chybové stavy, opět můžeme aplikaci rozšířit.

```
pub enum Error {
    CitizenAlreadyExists = 0,
    SenderNotFound = 1,
    ReceiverNotFound = 2,
    WrongPlatNumber = 3,
    SenderSameAsReceiver = 4,
}
```

Na závěr vytvoříme v kořenovém adresáři soubor `demo.rs`, ve kterém importujeme potřebné služby:

```
use exonum_cli::NodeBuilder;
use failure::Error;
use exonum_landregistry::contracts::LandregistryService;
```

Následně nám funkce `main` bude řídit běh celého programu:

```
fn main() -> Result<(), Error> {
    exonum::helpers::init_logger()?;
    NodeBuilder::development_node()?
        .with_default_rust_service(LandregistryService)
        .run()
}
```

Nyní si můžeme vyzkoušet funkčnost navrženého řešení. V souboru `tx_tests.rs` si vytvoříme zkušebního uživatele Alice a přidělíme jí číslo parcely 3528. K tomuto využijeme funkci `test_create_citizen()` a doplníme ji následujícím způsobem:

```
let citizen = get_citizen(&testkit, &tx.author());
assert_eq!(citizen.pub_key, tx.author());
assert_eq!(citizen.name, ALICE_NAME);
assert_eq!(citizen.plat_num, 3528);
```

Dále doplníme funkci `test_transfer()` o kód reprezentující převod parcely z Alice na Boba:

```
TxTransfer {
    new_num: 3528,
```

```
    seed: 0,
    to: bob.public_key(),
```

V příkazové řádce si najdeme cestu k našemu projektu a příkazem:

```
cargo run --example demo
```

spustíme aplikaci. V konzoli bychom měli vidět hlášení o úspěšně provedené transakci:

```
Transfer between citizens: Citizen { pub_key: PublicKey
   ↪ (070122b6...), name: "Alice", plat_num: 0 }
        => Citizen { pub_key: PublicKey(542eee3b...),
           ↪ name: "Bob", plat_num: 3528 }
```

Změnou parcelního čísla ve funkci `test_transfer()` se můžeme pokusit vyvolat různé chybové stavy a sledovat chování programu.

5.5 Závěr

- Zhodnoťte kvalitu navrženého řešení.
- Zkuste rozšířit aplikaci o libovolnou vlastní funkcionalitu.
- Jaké vidíte další využití technologie blockchain v praxi?

6 Návrh laboratorní úlohy – práce s knihovnou NoobChain

6.1 Cíl úlohy

Seznámit se s principem činnosti technologie blockchain. Pochopit princip provádění transakcí a vyzkoušet si vytvořit jednoduchou aplikaci.

6.2 Úkoly

1. Provést instalaci vývojového prostředí pro programovací jazyk Java.
2. Založit projekt a seznámit se se zdrojovými kódy knihovny NoobChain.
3. Dle přiloženého návodu naprogramovat funkční aplikaci.

6.3 Teoretický úvod

6.3.1 Technologie blockchain

Technologie blockchain obvykle odkazuje na transparentní a veřejně přístupnou účetní knihu, která umožňuje bezpečný převod jednotek cenin pomocí šifrování veřejným klíčem a pomocí proof-of-work (hodnota platebního prostředku se dokazuje vynaloženou prací).

6.3.2 Využití v praxi

Technologii blockchain si drtivá většina lidí spojuje výhradně s kryptoměnami (především s Bitcoinem). To by byl však velmi úzký úhel pohledu, neboť praktické nasazení je daleko širší. Odstavce níže uvádějí příklady nasazení blockchainu v praxi. Jedná se pouze o výběr. Obdobných aplikací existuje po celém světě spousta a mnohé další každým dnem vznikají.

Katastr nemovitostí v Gruzii

Správní úřad Gruzínské republiky používá technologii blockchain, aby poskytla svým občanům digitální osvědčení o jejich pozemku. Děje se tak, že přidá kryptografický důkaz o tom, že transakce byla zveřejněna v bitcoinovém blockchainu. Gruzínský správní úřad spolupracuje s Bitfuri Group, která poskytuje řešení založená na protokolu Bitcoin a tento projekt započal v dubnu 2016. Toto Gruzii pomáhá bojovat

proti korupci a řešit spory o majetkové nároky. Hlavním důvodem k použití blockchainu je zvýšit důvěryhodnost veřejnosti k vedení záznamů o majetku.

Ověřování akademických listin na Maltě

Maltská vláda spustila v říjnu 2017 projekt, který vyvíjí systém pro ověřování akademických listin využívající blockchain technologii. Maltské Ministerstvo školství a práce se rozhodlo využít Blockcerts, otevřený standard pro správu akademických záznamů. Blockerts zajišťuje všechny aspekty; vytváření, vystavování, prohlížení a ověřování certifikátů a využití blockchain technologie jako infrastruktury. Pilotní verze byla zahájena s cílem vytvořit ověřitelný důkaz vzdělání pro občany.

6.4 Pracovní postup

1. Provést instalaci vývojového prostředí pro programovací jazyk Java: Nainstalujeme si vývojové prostředí pro programování v jazyce Java. Tento návod je uzpůsoben pro vývojové prostředí Eclipse. Jeho instalaci nalezneme na adrese: `www.eclipse.org`. V sekci *Download* → *Download Packages* stáhneme *Eclipse IDE for Java Developers*. Stažený archiv rozbalíme.

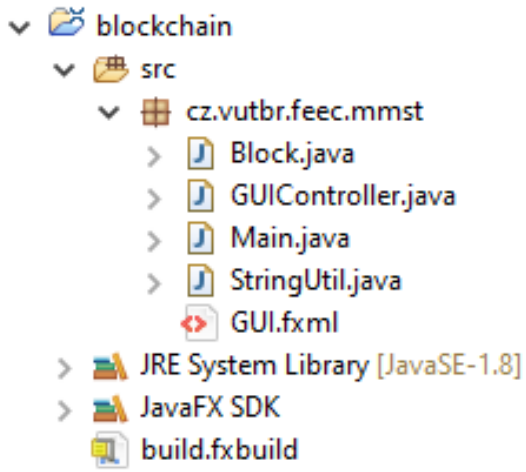
Dále si z webu Oracle (`www.oracle.com`) stáhneme JavaFX Scene Builder, který nám umožní tvorbu grafického rozhraní naší aplikace. Provedeme instalaci.

Zkontrolujeme aktuální stav nainstalovaných knihoven a v případě potřeby doinstalujeme základní nástroje pro vývoj aplikací pro platformu Java – JDK (Java Development Kit) a dále framework JavaFX pro vývoj grafického uživatelského rozhraní.

Otevřeme si vývojové prostředí Eclipse a propojíme jej s nástrojem Scene Builder. Zvolíme *Window* → *Preferences* → *JavaFX* a pomocí tlačítka *Browse...* vyhledáme spustitelný soubor *SceneBuilder.exe*.

2. Založit projekt a seznámit se se zdrojovými kódy knihovny NoobChain: Knihovna NoobChain se sestává z několika předpřipravených souborů zdrojových kódů, které lze díky srozumitelným komentářům snadno upravit na konkrétní příklad. My využijeme pouze jeden z nich a to *StringUtil.java*. Zbytek si doprogramujeme tak, aby odpovídal naší aplikaci. Zdrojovému kódu ze staženého souboru se pokusíme porozumět.

Založíme si nový JavaFX projekt a vhodně jej pojmenujeme. Ve složce zdrojových kódů vytvoříme potřebné soubory a zkopírujeme mezi ně i staženou část knihovny. Zkontrolujeme, případně doplníme, i připojení potřebných knihoven k projektu dle obr. 6.1.



Obr. 6.1: Struktura zdrojových souborů projektu

3. Dle přiloženého návodu naprogramovat funkční aplikaci: V následujících krocích si ukážeme, jak vytvořit jednoduchý katastr nemovitostí založený na blockchainu. Začneme editací souboru *Block.java*. Vytvoříme veřejnou třídu `Block` a v ní zadefinujeme potřebné proměnné. Proměnné volíme tak, aby odpovídaly účelu aplikace, např.:

```
private String parcelniCislo;
private String katastralniUzemi;
private String vymera;
private String vlastnik;
private String bpej;
public String hash;
public String previousHash;
private long timeStamp;
private int nonce;
```

Třídu doplníme o konstruktor a pokud bude později potřeba, tak i o příslušné `get`, `set` metody. Nyní napíšeme metodu `calculateHash`, která nám ze vstupních dat (v tomto případě jsou to proměnné, které jsme si zadefinovali výše) spočítá hash za pomoci metody `applySha256`, která je obsažená v souboru *StringUtil.java*.

```
public String calculateHash()
{
  String calculatedhash = StringUtil.applySha256(
      previousHash +
      Long.toString(timeStamp) +
      Integer.toString(nonce) +
      parcelniCislo +
```

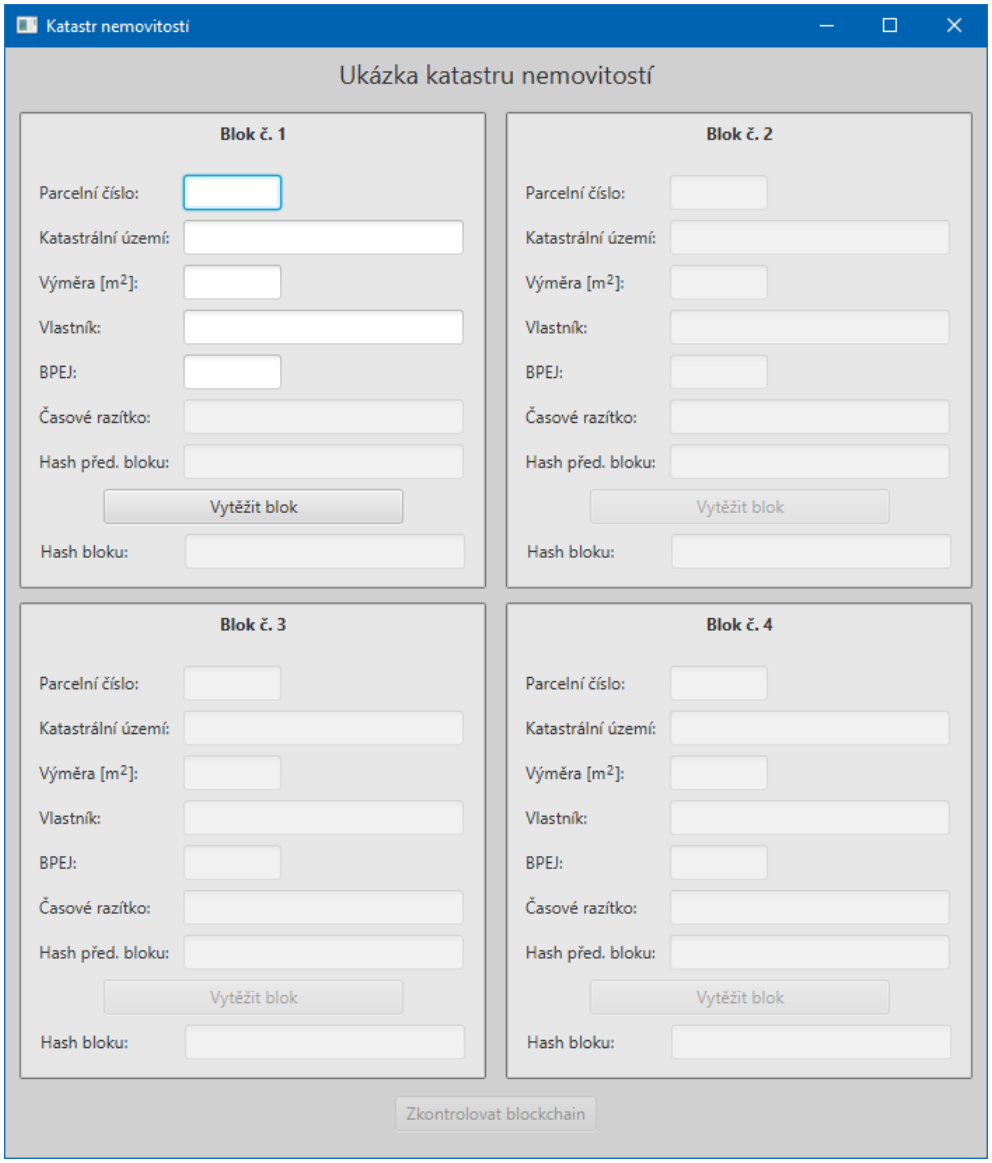
```
        katastralniUzemi +
        vymera +
        vlastnik +
        bpej
        );
    return calculatedhash;
}
```

Nyní se budeme věnovat tvorbě uživatelského rozhraní. Klikneme pravým tlačítkem myši na soubor *GUI.fxml* a vybereme možnost *Open with SceneBuilder*. Vytvoříme grafické rozhraní tak, aby odpovídalo obr. 6.2 a uvedené položky, aby korespondovaly s proměnnými zadefinovanými ve třídě `Block`.

Program bude fungovat tak, že uživatel vyplní údaje v jednom bloku a následně jej vytěží. Až po vytěžení předchozího bloku se mu zpřístupní formulářová políčka bloku následujícího. Současně s vytěžením bloku se deaktivuje příslušné tlačítko, aby se zabránilo vícenásobnému vytěžení téhož bloku. Po vytěžení posledního bloku se aktivuje tlačítko pro kontrolu celého blockchainu. V tomto smyslu také nastavíme vlastnost *Disable* u příslušných entit.

V souboru *GUIController.java* si musíme zadefinovat všechny prvky, které jsme použili v grafickém rozhraní. Příklad kódu pro první blok:

```
@FXML
private TextField parcelniCislo1;
@FXML
private TextField katastralniUzemi1;
@FXML
private TextField vymera1;
@FXML
private TextField vlastnik1;
@FXML
private TextField bpej1;
@FXML
private TextField casoveRazitko1;
@FXML
private TextField predchoziHash1;
@FXML
private TextField hash1;
@FXML
private Button vytezit1;
```



Obr. 6.2: Grafické rozhraní aplikace

Analogicky budeme postupovat i pro další tři bloky.

Nyní již zbývá jen naprogramovat metody, které budeme volat při stisku jednotlivých tlačítek. Příklad zdrojového kódu pro první tlačítko je uveden níže. Při stisku tlačítka vytvoříme pomocí konstruktoru nový objekt. Data pro jeho vytvoření získáme z formulářových políček, chybějící data dopočítáme (viz zdrojový kód). Následně u komponent příslušející druhému bloku odebereme vlastnost *Disable* a současně ji přidáme právě použitému tlačítku, abychom zabránili vícenásobnému vytěžení.

```
public void vytezit1Stisk(ActionEvent event)
{
  Block blok = new Block(parcelniCislo1.getText(),
     ↪ katastralniUzemi1.getText(), vymera1.getText(),
     ↪ vlastnik1.getText(), bpej1.getText(), "0");
  blockchain.add(blok);
  predchoziHash1.setText("0");
  predchoziHash2.setText(blockchain.get(0).hash);
  hash1.setText(blok.hash);
  casoveRazitko1.setText(Long.toString(blok.getTimeStamp
     ↪ ()));

  parcelniCislo2.setDisable(false);
  katastralniUzemi2.setDisable(false);
  vymera2.setDisable(false);
  vlastnik2.setDisable(false);
  bpej2.setDisable(false);
  vytezit2.setDisable(false);
  vytezit1.setDisable(true);
}
```

Analogicky postupujeme i v případě dalších tří tlačítek.

Poslední tlačítko (pro kontrolu celého blockchainu) bude fungovat tak, že si z formulářových políček načte vstupní data a pomocí metody `applySha256` spočítá hashe jednotlivých bloků. Ukázka zdrojového kódu pro kontrolní výpočet hashe prvního bloku:

```
String kontrolaHash1 = StringUtil.applySha256(
        "0" +
        Long.toString(blockchain.get(0).getTimeStamp()) +
        Integer.toString(blockchain.get(0).getNonce()) +
        parcelniCislo1.getText() +
```

```
        katastralniUzemi1.getText() +
        vymera1.getText() +
        vlastnik1.getText() +
        bpej1.getText()
        );
```

Takto spočítané hashe porovná s těmi, které se vypočítaly při těžené těch konkrétních bloků. V případě, že hashe nesouhlasí, jsme informování chybovou hláškou a kolizní hash je označen červeně. Pokud kontrola skončí úspěšně, jsme informováni hláškou, viz obr. 6.3. Příklad porovnání hashů prvního bloku je na výpisu níže. Opět provedeme analogicky i pro zbývající bloky.

```
if (!(kontrolaHash1.equals(blockchain.get(0).hash)))
{
  hash1.setStyle("-fx-text-fill: red;");
  vysledek.setText("Neúspěšná kontrola blockchainu");
  vysledek.setStyle("-fx-fill: red;");
}
```

Obr. 6.3: Možná hlášení aplikace o výsledku proběhlé kontroly

Na závěr se budeme věnovat spustitelnému souboru *Main.java*. Zde načteme soubor *GUI.fxml*, reprezentující grafické rozhraní. Nezapomene na ošetření možných chybových stavů.

```
Parent root = null;
try
{
  root = FXMLLoader.load(getClass().getResource("GUI.fxml
     ↪ "));
}
catch (IOException e)
```

```
{
  e.printStackTrace();
  return ;
}
```

A následně si definujeme renderovanou scénu.

```
Scene scene = new Scene(root);
primaryStage.setScene(scene);
primaryStage.setTitle("Katastr␣nemovitostí");
primaryStage.show();
```

Spustíme program a vyzkoušíme jej pro různé vstupy. Pokusíme se o vyvolání obou stavů výsledné kontroly blockchainu. Případné chyby, vzniklé při spuštění aplikace, se snažíme odstranit individuálně, např. za pomoci příslušné dokumentace.

6.5 Závěr

- Zhodnoťte kvalitu navrženého řešení.
- Zkuste upravit výslednou aplikaci na jinou oblast použití.
- Jaké vidíte další využití technologie blockchain v praxi?

Závěr

Cíle práce poskytnout přehledný a komplexní obraz o technologii blockchain jsme dosáhli v prvních dvou kapitolách. Cíle provést rozbor praktického nasazení bylo dosaženo ve třetí kapitole. Čtvrtá kapitola nám poskytuje důležité informace o dostupných open-source frameworcích, které využíváme v laboratorních úlohách. Praktickému výstupu se věnují poslední dvě kapitoly, jež jsou návrhy laboratorních úloh.

V první kapitole jsme se seznámili s technologií blockchain. Následující kapitola nám poskytla pohled na problematiku blockchainu z právního hlediska. Následující kapitola popsala případy praktického nasazení této technologie v různých nefinančních odvětvích. Další kapitola byla přehledem nejznámějších open-source frameworků a jejich stručného popisu. Poslední dvě kapitoly byly návrhem laboratorních úloh, kde byl kladem důraz na seznámení studentů s principem činnosti technologie blockchain.

Literatura

[1] MARR, B.: *35 Amazing Real World Examples Of How Blockchain Is Changing Our World* [online]. 2018 [cit. 11. 10. 2019]. Dostupné z URL: <https://www.forbes.com/sites/bernardmarr/2018/01/22/35-amazing-real-world-examples-of-how-blockchain-is-changing-our-world/#6158c8a343b5>

[2] *A Blockchain Platform for the Enterprise* [online]. 2019 [cit. 3. 12. 2019]. Dostupné z URL: <https://hyperledger-fabric.readthedocs.io/en/release-1.4/>

[3] FORTNEY, L.: *Bitcoin Mining, Explained* [online]. 2019 [cit. 17. 12. 2019]. Dostupné z URL: <https://www.investopedia.com/terms/b/bitcoin-mining.asp>

[4] CHROMAWAY: *Blockchain and Future House Purchases* [online]. 2018 [cit. 19. 10. 2019]. Dostupné z URL: <https://chromaway.com/landregistry/#oc%20-slider>

[5] ALLESSIE, D., SOBOLEWSKI, M., VACCARI, L., PIGNATELLI, F.: *Blockchain for digital government* [online]. 2019 [cit. 11. 10. 2019]. Dostupné z URL: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government>

[6] GRECH, A., CAMILLERI, A. F.: *Blockchain in Education* [online]. 2017 [cit. 23. 10. 2019]. Dostupné z URL: <https://www.pedocs.de/frontdoor.php?source_opus=15013>

[7] MERTENS, E.: *Blockchain Party*. Managing Intellectual Property 274. 2018 [cit. 24. 3. 2020]. Dostupné z URL: <https://www.pedocs.de/frontdoor.php?source_opus=15013>

[8] SEIDL, J.: *Blockchain pro začátečníky: Potvrzování a sledování transakcí – díl třetí* [online]. 2018 [cit. 15. 12. 2019]. Dostupné z URL: <https://www.dreport.cz/blog/blockchain-pro-zacatecniky-potvrzovani-a-sledovani-transakci-dil-treti/>

[9] *Blockchain Proofs* [online]. [cit. 31. 5. 2020]. Dostupné z URL: <https://wiki.p2pfoundation.net/Blockchain_Proofs>

[10] EUROPEAN COMMISSION: *Blockchain Technologies* [online]. 2019 [cit. 10. 12. 2019]. Dostupné z URL: <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>

[11] *Comment fonctionne la blockchain?* [online]. 2017 [cit. 19. 12. 2019]. Dostupné z URL: <https://coin24.fr/crypto-monnaies/dictionnaire/blockchain/>

[12] CONG, L. W., HE, Z., LI, J.: *Decentralized Mining in Centralized Pools* [online]. 2019 [cit. 13. 12. 2019]. Dostupné z URL: <https://www.nber.org/papers/w25592>

[13] *Developer Resources* [online]. 2019 [cit. 2. 12. 2019]. Dostupné z URL: <https://ethereum.org/developers/>

[14] SNIP, I.: *Georgia: Authorities Use Blockchain Technology for Developing Land Registry* [online]. 2017 [cit. 15. 10. 2019]. Dostupné z URL: <https://eurasianet.org/georgia-authorities-use-blockchain-technology-for-developing-land-registry>

[15] BOUCHER, P., NASCIMENTO, S., KRITIKOS, M.: *How blockchain technology could change our lives* [online]. 2017 [cit. 19. 10. 2019]. Dostupné z URL: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf>

[16] HAYES, A.: *How Does Bitcoin Mining Work?* [online]. 2019 [cit. 15. 12. 2019]. Dostupné z URL: <https://www.investopedia.com/tech/how-does-bitcoin-mining-work/>

[17] LEONG, L.: *Intro to Bitcoin, Blockchain, and Mining with some Python* [online]. 2019 [cit. 15. 12. 2019]. Dostupné z URL: <https://towardsdatascience.com/intro-to-bitcoin-blockchain-and-mining-with-some-python-ee0765b6079b>

[18] HARAŠTA, J.: *Konzultace s odborným asistentem Ústavu práva a technologií, Právnická fakulta, Masarykova univerzita.* Brno [cit. 2. 3. 2020].

[19] HORÁK, M.: *Konzultace s odborným pracovníkem Bezpečnostního týmu, CSIRT, Masarykova univerzita.* Brno [cit. 16. 3. 2020].

[20] POLČÁK, R.: *Konzultace s vedoucím Ústavu práva a technologií, Právnická fakulta, Masarykova univerzita.* Brno [cit. 6. 3. 2020].

[21] LYONS, T., COURCELAS, L., TIMSIT, K.: *Legal and regulatory framework of blockchains and smart contracts* [online]. 2019 [cit. 18. 3. 2020]. Dostupné z URL: <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf>

[22] MICALLEF, K.: *Malta begins multiyear roll out of Blockcerts* [online]. 2019 [cit. 17. 10. 2019]. Dostupné z URL: <https://maltablockchainsummit.com/news/malta-begins-multiyear-roll-out-of-blockcerts/>

[23] KESZTHELYI, CH.: *Malta to issue blockchain certificates for students* [online]. 2019 [cit. 17. 10. 2019]. Dostupné z URL: <https://businessmalta.com/malta-to-issue-blockchain-certificates-for-students/1513/>

[24] SIMPSON, I.: *More digital ID from uPort and SBB* [online]. 2018 [cit. 21. 10. 2019]. Dostupné z URL: <https://cryptovalley.swiss/digital-id-from-uport-and-sbb/>

[25] BARAN, P.: *On Distributed Communications Networks* [online]. 1962 [cit. 19. 12. 2019]. Dostupné z URL: <https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf>

[26] *Proof of Stake* [online]. [cit. 31. 5. 2020]. Dostupné z URL: <https://wiki.p2pfoundation.net/Proof_of_Stake>

[27] *Proof of work* [online], poslední aktualizace 24. 4. 2019, Bitcoin Wiki. Dostupné z URL: <https://en.bitcoin.it/wiki/Proof_of_work>

[28] TAR, A.: *Proof-of-Work, Explained* [online]. 1962 [cit. 31. 5. 2020]. Dostupné z URL: <https://cointelegraph.com/explained/proof-of-work-explained>

[29] *Quorum – Enterprise Ethereum Client* [online]. 2019 [cit. 4. 12. 2019]. Dostupné z URL: <https://docs.goquorum.com/en/latest/>

[30] SINGH, N.: *Swiss Government Using uPort to Register Zug Citizens* [online]. 2018 [cit. 21. 10. 2019]. Dostupné z URL: <https://hackernoon.com/swiss-government-using-uport-to-register-zug-citizens-b71290caa798>

[31] SMOLENSKI, N.: *Take your learning with you* [online]. 2018 [cit. 17. 10. 2019]. Dostupné z URL: <https://timesofmalta.com/articles/view/Take-your-learning-with-you.678403>

[32] SWISH LABS, kolektiv autorů: *The 5 best blockchain platforms for enterprises and what makes them a good fit* [online]. 2019 [cit.

17. 11. 2019]. Dostupné z URL: <https://medium.com/swishlabs/the-5-best-blockchain-platforms-for-enterprises-and-what-makes-them-a-good-f

[33] BITFURY, kolektiv autorů: *The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project* [online]. 2017 [cit. 15. 10. 2019]. Dostupné z URL: <https://medium.com/@BitfuryGroup/the-bitfury-group-and-government-of-republic-of-georgia-expand-historic-bloc

[34] SHIN, L.: *The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project* [online]. 2017 [cit. 15. 10. 2019]. Dostupné z URL: <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands#38d24c504dcd>

[35] CHROMAWAY: *The Land Registry in the blockchain – testbed* [online]. 2017 [cit. 19. 10. 2019]. Dostupné z URL: <https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf>

[36] MARUŠIN, M.: *Virtual Wallet Compatible with Cryptocurrency*. Brno, 2018. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Mgr. Ing. Pavel Očenášek, Ph.D.

[37] *Welcome to Corda!* [online]. 2018 [cit. 5. 12. 2019]. Dostupné z URL: <https://docs.corda.net/>

[38] ETHEREUM: *Welcome to the Ethereum Wiki!* [online]. 2019 [cit. 2. 12. 2019]. Dostupné z URL: <https://github.com/ethereum/wiki/wiki>

[39] RAJ, R.: *What is Blockchain Mining?* [online]. 2019 [cit. 17. 12. 2019]. Dostupné z URL: <https://intellipaat.com/blog/tutorial/blockchain-tutorial/what-is-bitcoin-mining/>

[40] ALYSON: *What is blockchain technology?* [online]. 2019 [cit. 10. 12. 2019]. Dostupné z URL: <https://support.blockchain.com/hc/en-us/articles/211160223-What-is-blockchain-technology->

[41] SHARMA, T. K.: *What is Quorum Blockchain?* [online]. 2018 [cit. 4. 12. 2019]. Dostupné z URL: <https://www.blockchain-council.org/blockchain/what-is-quorum-how-is-it-different-from-other-blockchain/>

[42] *Zug Digital ID: Blockchain Case Study for Government Issued Identity* [online]. 2019 [cit. 21. 10. 2019]. Dostupné z URL: <https://consensys.net/enterprise-ethereum/use-cases/government-and-the-public-sector/zug/>